802.11b and associated network security risks for the home user

by Michael Osten mosten@bleepyou.com

Background

Approved in 1997 by the IEEE 802 committee, 802.11 details the framework necessary for a standard method of wireless networked communications. 802.11 uses the 2.4-GHz microwave band designated for low-power unlicensed use by the FCC in the USA in 1985.

It allows for two distinct methods of encoding, FHSS and DSSS. FHSS (Frequency Hopping Spread Spectrum) distributes the communication across 75 one-MHz subchannels, randomly skipping between them.

Two operating modes are defined: infrastructure and ad hoc. Dedicated hardware (the access point) provides a basic or extended service set that builds the wireless infrastructure. It provides basic bridging, as well as allowing clients to roam from access point to access point (provided they all exist on the same ethernet segment; roaming across subnets is not possible at this time). The ad hoc (IBSS, or Independent Basic Service Set) mode allows individual nodes to participate in a peer-to-peer network without an access point.

DSSS (Direct Sequence Spread Spectrum) breaks the band into 14 overlapping 22-MHz channels and uses one channel at a time.

In September of 1999, the 802 committee extended the specification, deciding to standardize on DSSS. This extension, 802.11b, allowed for new, more exotic encoding techniques. This pushed up the throughput to a much more respectable 5.5 Mbps (up to 11 Mbps). While breaking compatibility with FHSS schemes, the new extensions made it possible for new equipment to continue to interoperate with older 802.11 DSSS hardware.

The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from interception. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP. WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless ethernet card) and an access point (ie. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe; however, no commercial system I am aware of has mechanisms to support such techniques.

Problem

=========

802.11b is an increasingly common method of distributing network connectivity to mobile users in both the workplace and the home. Unlike corporate users, little attention has been paid by home users to the security of personal wireless networks.

Most consumer hardware access points have WEP capabilities, but as my research has shown very few home wireless "administrators\enable WEP, disable broadcast of SSID, or even change the default settings that shipped from the factory.

Even with WEP enabled, users can not be certain of network security as outlined in "Security of the WEP algorithm\u" paper detailing the faults of WEP's RC4 encryption algorithm It has become fairly trivial to break WEP with several hours of wireless sniffing with software designed for this purpose. (See Resources)

This oversight leaves users open to unauthorized access to internal privileged information, as well as an unauthorized use of network services.

Research

802.11 Access point detection:

Over the course of several days I have mapped hundreds of residential and business wireless access points in the Ft. Lee/Jersey City/Hoboken New Jersey areas. (see figure 1-3). All captures were from a car traveling at hiway speeds. Less than 2 percent have enabled WEP. Less than 20 percent have changed the default SSID from factory settings. This causes a problem in that a person with a small amount of hardware can hijack broadband connection with total anonymity from a car, or an apartment across the street. All data presented here was collected with a Compaq Ipaq and Windows CE with a Lucent WavLan 802.11b WIFI card running Ministumber (See Resources).

Pocket_PC		
File Zoom Tools	Help	
🏽 MiniStumbler	8	:32a
MAC	SSID	-
O0045A267A51	tamapp	=
○ 00045ACE19EB	linksys	
O0501806CD80	daphnedoll	
00045ACE3CE7	linksys	
00045A2FDB9D	linksys	
00045AEE5CEB	overtherainbow	
O00625517CCE	ASDFGHJK	
00022D068A9C	068a9c	
0050180913FE	AirCIDD	
00045AECDF53	linksys	
00904B083132	hervehome	
00045AE82779	linksys	
	Wireless	-
	1	•
Ready Not sca	annir GPS Off	115
File View Opt Spd	GPS Þ 🚯	₩

Figure 1 (Ministumber displaying detected SSID's)

WEP and weakness of RC4 key scheduling:

All data presented here was collected with a Sony Viao using a D-Link Prism2 based 802.11b card, and Linux using "Kismet\ "Ethereal\and \AirSnort\See Resources) to demonstrate breaking WEP. All data collected in the attempt to demonstrate the weakness of WEP originated from my personal network.

There are several dangers to having not enabled WEP. Although WEP has proven insecure, it still provides a deterrent for all but the most determined intruder.

Figure 3 and 4 show what happens when 802.11b traffic is sniffed using Kismet and Ethereal. All packets are logged, and all plain text login/passwords (telnet, pop3, ect) are clearly shown by looking through the logs as displayed by Ethereal. As well as traffic history, what websites you have visited, etc.

🙋 mosten@vi	ao.bleepyou.	com: /home/mosten	- • ×
File Ed	it Settings	Help	
₽-Networks- SSID ! makoree 	f	T W Ch Data LLC Crypt Wk Flags A N 06 457 77 0 0 A3	Info
 			Elapsd 000023 = _JH_M_S_J
Status Found SSI Found IP Detected Logging d	D "makoreef" range for "< new network ata networks	for cloaked network BSSID 00:40:96:42:D8:7C no ssid>" via ARP 172.16.0.0 " <no ssid="">" bssid 00:40:96:42:D8:7C WEP N Ch weak cisco</no>	6

Figure 3 (Kismet monitoring non WEP enabled network)

Eile Eile Gapture Display Tools No., Time Source Destination Protocol Info 50 1.007790 Repre_2d182:ee Protocol AFP 172,16,0,233 is at 00:02:2d:2d:82:ee 51 1.027781 Repre_2d182:ee Protocol AFP 172,16,0,233 is at 00:02:2d:2d:82:ee 52 1.047782 Repre_2d182:ee PRPre_0d186:ee AFP Mon has 172,16,0,233 is at 00:02:2d:2d:82:ee 53 1.067777 O0:8e:ef:ed:9e:00 Repre_0d186:ef AFP Win has 172,16,0,2357 Tell 172,16,0,1 54 1.067773 Rironet_42:d8:7c RN IEEE 902,11 Acknowledgement 55 1.17776 Repre_00:f8:47 AFP Who has 172,16,0,2357 Tell 172,16,0,1 61 1.227791 O0:8e:ef:ed:9e:00 Repre_02:74:cf AFP Who has 172,16,0,2267 Tell 172,16,0,1 61 1.227791 O0:8e:ef:ed:9e:00 Repre_2d18:7c RP Who has 172,16,0,2267 Tell 172,16,0,1 62 1.247767 Repre_2d18:7c	-02	Eile Edit Capture Display Tools							
No. Time Source Destination Protocol Info 50 1.007750 Agere_2d182:ee Protocol Here 902.11 Hershouledgement 51 1.027781 Agere_2d182:ee Protocol APP 172.16.0.233 is at 00:02:2d12d:82:ee 53 1.067767 00:8e:ef:ed:9e:00 APP 172.16.0.254? Tell 172.16.0.1 54 1.067773 Aircnet_42:d8:7c RAP Who has 172.16.0.254? Tell 172.16.0.1 54 1.067775 00:8e:ef:ed:9e:00 Agere_08:b3:05 APP Who has 172.16.0.257? Tell 172.16.0.1 55 1.107776 Agere_08:b3:05 RAP Who has 172.16.0.235? Tell 172.16.0.1 55 1.107776 Agere_09:F8:47 APP Who has 172.16.0.235? Tell 172.16.0.1 59 1.187055 00:8e:ef:ed:9e:00 Agere_06:74:cf RAP Who has 172.16.1.244? Tell 172.16.0.1 61 1.227791 00:8e:ef:ed:9e:00 Agere_06:74:cf APP Who has 172.16.0.226? Tell 172.16.0.1 61 1.227781 <t< th=""><th>Help</th></t<>	Help								
sol pggre_0distion Pggre_0distion Pggre_0distion 51 1.027781 Aggre_2distice Apgre_0distion APP 172.16.0.233 is at 00:02:2distice 52 1.047782 Apgre_0disticn APP Unknowledgement 53 1.067767 00:8e:ef:ed:9e:00 APP Who has 172.16.0.254? Tell 172.16.0.1 54 1.067777 O0:8e:ef:ed:9e:00 Agere_08:b3:05 APP Who has 172.16.0.254? Tell 172.16.0.1 54 1.067778 Aironet_d2:d8:7c (RA) IEEE 902.11 Acknowledgement 55 1.107781 Agere_09:b3:05 RA) IEEE 902.11 Acknowledgement 55 1.107781 Agere_09:b3:05 RA) IEEE 902.11 Acknowledgement 56 1.12776 Agere_09:b3:05 RA) IEEE 902.11 Acknowledgement 57 1.147770 00:8e:ef:ed:9:00 Agere_00:F8:47 APP Who has 172.16.0.235? Tell 172.16.0.1 61 1.227781 00:8e:ef:ed:9:00 Agere_00:F2:22:3f APP Who has 172.16.1.244?		Info	Protocol	Destination	Source	Time	10		
51 1.027781 Agere_2d:82:ee 00:80:ef;ed:99:00 AFP 172.16.0.233 is at 00:02:2d:2d:2d:2d:2d:2d:2d:2d:2d:2d:2d:2d:2d	_	Hoknowledgenent	TEEE 802.11	HOGLETOGIZETON (HH)		1,007790	50		
52 1,047782 Agere_23t32tec (PA) IEEE 302.11 Acknowledgement 53 1,067767 00:8e:ef:ed:9e:00 Agere_03:b3:05 AFP Who has 172.16.0.254? Tell 172.16.0.1 54 1,067773 Airconet_42:d8:7c (RA) IEEE 302.11 Acknowledgement 55 1,107781 Airconet_42:d8:7c (RA) IEEE 302.11 Acknowledgement 56 1,127776 Agere_03:b3:05 (RA) IEEE 302.11 Acknowledgement 57 1,147770 Agere_03:b3:05 (RA) IEEE 302.11 Acknowledgement 58 1.16310 Agere_00:f8:47 AFP Who has 172.16.0.2357 Tell 172.16.0.1 59 1,187885 00:8e:ef:ed:9e:00 Agere_00:f8:47 AFP Who has 172.16.1.244? Tell 172.16.0.1 60 1,207778 Airconet_42:d8:7c (RA) IEEE 302.11 Acknowledgement Agere_00:f4:47 AFP Who has 172.16.1.244? Tell 172.16.0.1 61 1,227791 00:9e:ef:ed:9e:00 Agere_0/2:74:cf AFP Who has 172.16.1.242? Tell 172.16.0.1 61 1,227780 00:9e:ef:ed:9e:00 Agere_0/2:74:cf AFP Who has 172.16.0.226? Tell 172.16.0.1 62 1,247767 O0:9e:ef:ed:9e:00 Agere_0/2:22:37 AFP Who has 172.16.0.226? Tell 172.16.0.1		172.16.0.233 is at 00:02:2d:2d:82:ee	ARP	00:8e:ef:ed:9e:00	Agene_2d:82:ee	1.027781	51		
53 1,067767 00;8e;ef;ed;9e;00 Agere_03;b3;05 AFP Who has 172,16,0,2547 Tell 172,16,0,1 54 1,067773 Aironet_42;d8;7c (RA) IEEE 902,11 Acknowledgement 55 1,107781 Aironet_42;d8;7c (RA) IEEE 902,11 Acknowledgement 56 1,127776 Agere_03;b3;05 (RA) IEEE 902,11 Acknowledgement 57 1,147770 00;8e;ef;ed;9e;00 Agere_03;b3;05 (RA) IEEE 902,11 Acknowledgement 59 1,187885 00;8e;ef;ed;9e;00 Agere_00;f8;47 AFP Who has 172,16,0,2357 Tell 172,16,0,1 60 1,207778 Aironet_42;d8;7c (RA) IEEE 902,11 Acknowledgement Aironet_42;d8;7c (RA) IEEE 902,11 Acknowledgement 61 1,227791 00;8e;ef;ed;9e;00 Agere_00;74;cf AFP Who has 172,16,0,2567 Tell 172,16,0,1 62 1,247767 Aironet_42;d8;7c (RA) IEEE 902,11 Acknowledgement Agere_00;74;cf AFP Who has 172,16,0,2267 Tell 172,16,0,1 64 1,287765 Lucent_f2;22;37 AFP Who has 172,16,0,2267 Tell 172,16,0,1 Agere_00;74;cf AFP Who has 172,16,0,2267 Tell 172,16,0,1 65 1,307767 Lucent_f2;22;37 AFP <		Acknowledgement	IEEE 802.11	Agene_2d:82:ee (RA)	าสัมธรรมการสาวสาว	1,047782	52		
54 1,067773 Aironet_422dB;7c (RA) IEEE 802,11 Acknowledgement 55 1,107781 Rironet_422dB;7c (RA) IEEE 802,11 Acknowledgement 56 1,127776 Agere_08;53;05 (RA) IEEE 802,11 Acknowledgement 57 1,147770 00;8e;ef;ed;9e;00 Agere_00;f8;47 ARP Who has 172,16,0,235? Tell 172,16,0,1 58 1,187885 00;8e;ef;ed;9e;00 Lucent_f2;22;37 ARP Who has 172,16,1,244? Tell 172,16,0,1 60 1,207778 Rironet_42;d8;7c (RA) IEEE 802,11 Acknowledgement Rironet_42;d8;7c (RA) IEEE 802,11 Acknowledgement 61 1,227791 00;8e;ef;ed;9e;00 Agere_06;74;cf ARP Who has 172,16,1,244? Tell 172,16,0,1 62 1,247767 Rironet_42;d8;7c (RA) IEEE 802,11 Acknowledgement Rironet_42;d8;7c (RA) IEEE 802,11 Acknowledgement 63 1,267788 00;8e;ef;ed;9e;00 Agere_2d;82;fe ARP Who has 172,16,1,242? Tell 172,16,0,1 64 1,287765 Lucent_f2;22;37 00;8e;ef;ed;9e;00 ARP 172,16,1,244 is at 00;60;1d;f2;22;3f 65 1,307767 Lucent_f2;22;37 RAP Who has 172,16,0,225? Tell 172,16,0,1 10 EEE 802,11 Lucent_f2;22;37 IEEE 802,11 Acknowledgement IEEE 802,11 Lucent_f2;22;37 RAP JANNOWLED JANNOWLED IEEE 802,11		Who has 172.16.0.254? Tell 172.16.0.1	ARP	Agene_08:b3:05	00;8e:ef:ed:9e:00	1,067767	53		
55 1,107781 Aironet_42;d0;7c (RA) IEEE 002,11 Acknowledgement 56 1,127776 Negere_00;b3;05 (RA) IEEE 002,11 Acknowledgement 57 1,147770 00;8e;ef;ed;9e;00 Agere_00;f8;47 AFP Who has 172,16,0,235? Tell 172,16,0,1 58 1,169310 Aironet_42;d0;7c (RA) IEEE 002,11 Acknowledgement Locent_f2;22;37 AFP Who has 172,16,1,244? Tell 172,16,0,1 50 1,207778 Aironet_42;d0;7c (RA) IEEE 002,11 Acknowledgement Locent_f2;22;37 AFP Who has 172,16,1,252? Tell 172,16,0,1 61 1,207778 Aironet_42;d0;7c (RA) IEEE 002,11 Acknowledgement Aironet_42;d0;7c (RA) IEEE 002,11 Acknowledgement 61 1,227791 00;8e;ef;ed;9e;00 Agere_06;74;cf AFP Who has 172,16,0,226? Tell 172,16,0,1 62 1,247767 Aironet_42;d0;7c (RA) IEEE 002,11 Acknowledgement Aironet_42;d0;7c (RA) IEEE 002,11 Acknowledgement 63 1,267785 Lucent_f2;22;37 O0;8e;ef;ed;9e;00 AFP J72,16,1,244 is at 00;60;1d;f2;22;37 64 1,287767 Lucent_f2;22;37 (RA) IEEE 002,11 Acknowledgement IEEE 002,11 Acknowledgement IEEE 002,11 Acknowledgement 11 Cogical-Link Control Address Resolution Protocol (request) AFP J72,16,1,244 is at 00;60;1d;f2;22;37 10 00 8e ef ed 9e 00 70 E8 as as 03 00 00 00 08 06 ,0000 99,0,0,800 J80 <td></td> <td>Acknowledgement</td> <td>IEEE 802,11</td> <td>Aironet_42:d8:7c (RA)</td> <td></td> <td>1,087773</td> <td>- 54</td>		Acknowledgement	IEEE 802,11	Aironet_42:d8:7c (RA)		1,087773	- 54		
56 1.127776 Agere_08;b3;05 (RA) IEEE 902,11 Acknowledgement 57 1.147770 00;8e:ef:ed:9e:00 Agere_00;f8;47 ARP Who has 172,16,0,2357 Tell 172,16,0,1 58 1.169310 Aironet_42:d8;7c (RA) IEEE 902,11 Acknowledgement ARP Who has 172,16,1,2447 Tell 172,16,0,1 59 1.187885 00;8e:ef:ed:9e:00 Lucent_f2:22:37 ARP Who has 172,16,1,2447 Tell 172,16,0,1 60 1.207778 Aironet_42:d8;7c (RA) IEEE 802,11 Acknowledgement Aironet_42:d8;7c (RA) IEEE 902,11 Acknowledgement 61 1.227791 00;8e:ef:ed:9e:00 Agere_00;74;cf ARP Who has 172,16,0,2267 Tell 172,16,0,1 62 1.247767 Aironet_42:d8;7c (RA) IEEE 902,11 Acknowledgement Aironet_42:d8;7c (RA) IEEE 902,11 Acknowledgement 63 1.267788 00:8e:ef:ed:9e:00 Agere_2d:82;fe ARP Who has 172,16,0,2267 Tell 172,16,0,1 64 1.287765 Lucent_f2:22:3f CRA IEEE 902,11 Acknowledgement 100:8e:ef:ed:9e:00 ARP 172,16,1,244 is at 00;60;1d;f2:22;3f Locent_f2:22:3f (RA) IEEE 902,11 Acknowledgement Visition Protocol (request) Address Resolution Protocol (req		Acknowledgement	IEEE 802,11	Aironet_42;d8;7c (RA)		1,107781	55		
57 1.147770 00:8e:ef:ed:9e:00 Agere_00:f8:47 ARP Who has 172.16.0.235? Tell 172.16.0.1 58 1.169310 Atronet_42:d8:7c (RA) IEEE 802.11 Acknowledgement 59 1.187885 00:8e:ef:ed:9e:00 Lucent_f2:22:3f ARP Who has 172.16.1.247? Tell 172.16.0.1 60 1.207778 00:8e:ef:ed:9e:00 Agere_06:74:cf ARP Who has 172.16.1.247? Tell 172.16.0.1 61 1.207778 00:8e:ef:ed:9e:00 Agere_06:74:cf ARP Who has 172.16.1.247? Tell 172.16.0.1 62 1.247767 Aironet_42:d8:7c (RA) IEEE 802.11 Acknowledgement 63 1.267789 00:8e:ef:ed:9e:00 Agere_2d:82:fe ARP Who has 172.16.0.226? Tell 172.16.0.1 64 1.287765 Lucent_f2:22:3f (RA) IEEE 802.11 Acknowledgement 765 1.307767 Ucent_f2:22:3f (RA) IEEE 802.11 Acknowledgement 77 1.2827765 Lucent_f2:22:3f (RA) IEEE 802.11 Acknowledgement 78 1.307767 Lucent_f2:22:3f (RA) IEEE 802.11 </td <td></td> <td>Acknowledgement</td> <td>IEEE 902.11</td> <td>Agene_08;b3;05 (RA)</td> <td></td> <td>1,127776</td> <td>56</td>		Acknowledgement	IEEE 902.11	Agene_08;b3;05 (RA)		1,127776	56		
58 1.169310 Aironet_42:d8:7c (RA) IEEE 802.11 Acknowledgement 59 1.187885 00:8e:ef:ed:9e:00 Lucent_f2:22:37 AFP Who has 172.16.1.244? Tell 172.16.0.1 60 1.207778 Aironet_42:d8:7c (RA) IEEE 802.11 Acknowledgement 61 1.227791 00:8e:ef:ed:9e:00 Agere_0b:74:cf AFP Who has 172.16.1.252? Tell 172.16.0.1 62 1.247767 Aironet_42:d8:7c (RA) IEEE 802.11 Acknowledgement 63 1.267788 00:8e:ef:ed:9e:00 Agere_2d:82:fe AFP Who has 172.16.0.226? Tell 172.16.0.1 64 1.287765 Lucent_f2:22:37 Agere_2d:82:fe AFP Who has 172.16.0.226? Tell 172.16.0.1 65 1.307767 O:8e:ef:ed:9e:00 AFP 172.16.1.244 is at 00:60:1d:f2:22:3f 65 1.307767 Lucent_f2:22:3f (RA) IEEE 802.11 Acknowledgement 7 Visetfiel:9e:00 AFP 172.16.1.244 is at 00:60:1d:f2:22:3f 1 Lucent_f2:22:3f (RA) IEEE 802.11 Acknowledgement 7 Ucent_f2:22:3f (RA) IEEE 802.11 Acknowledgement 1 Address Resolution Protocol (request) 000 08 02 00 00 ff ff ff ff ff ff ff 00 40 96 42 d8 7c		Who has 172.16.0.235? Tell 172.16.0.1	ARP	Agene_00:f8:47	00:8e:ef:ed:9e:00	1,147770	-57		
59 1.187885 00:8e:ef:ed:9e:00 Lucent_f2:22:3f ARP Who has 172.16.1.244? Tell 172.16.0.1 60 1.207778 Aironet_42:d8:7c (RA) IEEE 802.11 Acknowledgement 61 1.227791 00:8e:ef:ed:9e:00 Agere_0b:74:ef ARP Who has 172.16.1.252? Tell 172.16.0.1 62 1.247767 Aironet_42:d8:7c (RA) IEEE 902.11 Acknowledgement 63 1.267788 00:8e:ef:ed:9e:00 Agere_0b:74:ef ARP Who has 172.16.0.226? Tell 172.16.0.1 64 1.287765 Lucent_f2:22:3f OO:8e:ef:ed:9e:00 ARP IFEE 802.11 65 1.307767 Lucent_f2:22:3f (RA) IEEE 802.11 Acknowledgement 1/Frame 1 (78 on wire, 78 captured) IEEE 802.11 Acknowledgement 1/20jcal-Link Control Address Resolution Protocol (request) Address Resolution Protocol (request) 000 08 02 00 00 ff ff ff ff ff ff ff 00 40 96 42 d8 7c		Acknowledgement	IEEE 802.11	Aironet_42:d8:7c (RA)		1,169310	58		
60 1,207778 Aironet_42;d8;7c (RA) IEEE 802,11 Acknowledgement 61 1,227791 00;8e;ef;ed;9e;00 Agere_0b;74;cf ARP Who has 172,16,1,2527 Tell 172,16,0,1 62 1,247767 Aironet_42;d8;7c (RA) IEEE 802,11 Acknowledgement Aironet_42;d8;7c (RA) IEEE 902,11 Acknowledgement 63 1,267788 00;8e;ef;ed;9e;00 Agere_0b;74;cf ARP Who has 172,16,0,2267 Tell 172,16,0,1 64 1,287765 Lucent_f2;22;3f 00;8e;ef;ed;9e;00 ARP 172,16,1,244 is at 00;60;1d;f2;22;3f 65 1,307767 Lucent_f2;22;3f (RA) IEEE 802,11 Acknowledgement 172,16,1,244 is at 00;60;1d;f2;22;3f 1 Frame 1 (78 on wire, 78 captured) IEEE 802,11 IEEE 802,11 1 Logical-Link Control Address Resolution Protocol (request)		Who has 172,16,1,244? Tell 172,16,0,1	ARP	Lucent_f2:22:3f	00;8e:ef:ed:9e:00	1,187885	59		
61 1,227791 00:8e:ef;ed;9e:00 Agere_0b:74:cf ARP Who has 172,16,1,2527 Tell 172,16,0,1 62 1,247767 Aironet_42:d8:7c (RA) IEEE 902,11 Acknowledgement 63 1,267788 00:8e:ef;ed:9e:00 Agere_2d:82:fe APP Who has 172,16,0,267 Tell 172,16,0,1 64 1,287765 Lucent_f2:22:3f 00:8e:ef:ed:9e:00 APP 172,16,1,244 is at 00:60:1d:f2:22:3f 65 1,307767 Lucent_f2:22:3f (RA) IEEE 802,11 Acknowledgement IEEE 802,11 Logaical-Link Control Iddress Resolution Protocol (request) Address Resolution Protocol (request) 00 08 02 00 00 ff ff ff ff ff ff ff 00 40 96 42 d8 7c		Acknowledgement	IEEE 802,11	Aironet_42:d8:7c (RA)		1,207778	60		
62 1,247767 Aironet_42:d8:7c (RA) IEEE 002,11 Acknowledgewent 63 1.267788 00:8e:ef:ed:9e:00 Agere_2d:82:fe AFP Who has 172.16.0.2267 Tell 172.16.0.1 64 1.287765 Lucent_f2:22:3f 00:8e:ef:ed:9e:00 ARP 172.16.1.244 is at 00:60:1d:f2:22:3f 65 1.307767 Lucent_f2:22:3f (RA) IEEE 002,11 Acknowledgewent Frame 1 (78 on wire, 78 captured) IEEE 802.11 Logical-Link Control Address Resolution Protocol (request) 00 08 02 00 00 ff ff ff ff ff ff ff ff ff f0 0 40 96 42 d8 7c		Who has 172,16,1,2527 Tell 172,16,0,1	ARP	Agene_0b:74:cf	00;8e;ef;ed;9e;00	1,227791	61		
63 1.267788 00:8e:ef:ed:9e:00 Agere_2d:82:fe ARP Who has 172.16.0.226? Tell 172.16.0.1 64 1.287765 Lucent_f2:22:3f 00:8e:ef:ed:9e:00 ARP 172.16.1.244 is at 00:60:1d:f2:22:3f 65 1.307767 Lucent_f2:22:3f (RA) IEEE 802.11 Acknowledgewent Frame 1 (78 on wire, 78 captured) IEEE 802.11 Logical-Link Control Address Resolution Protocol (request)		Acknowledgement	IEEE 902,11	Aironet_42;d8;7c (RA)		1,247767	62		
64 1.287765 Lucent_f2:22:3f 00:8e:ef:ed:9e:00 ARP 172.16.1.244 is at 00:60:1d:f2:22:3f 65 1.307767 Lucent_f2:22:3f (RA) IEEE 802.11 Acknowledgement Frame 1 (78 on wire, 78 captured) IEEE 802.11 Logical-Link Control Address Resolution Protocol (request)		Who has 172.16.0.226? Tell 172.16.0.1	ARP	Agene_2d:82:Fe	00:8e:ef:ed:9e:00	1,267788	63		
65 1,307767 Lucent_f2:22:3f (RR) IEEE 802,11 Acknowledgewent Frame 1 (78 on wire, 78 captured) IEEE 802,11 Logical-Link Control Address Resolution Protocol (request) 00 08 02 00 00 ff ff ff ff ff ff ff ff f0 040 96 42 d8 7c 10 00 8e ef ed 9e 00 70 68 as as 03 00 00 00 08 05 20 00 01 08 00 06 04 00 01 00 Re ef ef 9e 00 as 10		172.16.1.244 is at 00:60:1d:f2:22:3f	ARP	00:8e:ef:ed:9e:00	Lucent_f2:22:3f	1,287765	64		
Frame 1 (78 on wire, 78 captured) IEEE 802.11 Logical-Link Control Address Resolution Protocol (request) 00 08 02 00 00 ff ff ff ff ff ff f00 40 96 42 d8 7c		Acknowledgement	IEEE 802,11	Lucent_f2:22:3f (RA)		1,307767	65		
I Frame 1 (78 on wire, 78 captured) I EEE 802.11 Logical-Link Control Address Resolution Protocol (request) 00 08 02 00 00 ff ff ff ff ff ff 00 40 96 42 d8 7c	2						_		
000 08 02 00 00 ff ff ff ff ff ff ff 00 40 96 42 d8 7c				t)	n wire, 78 captured) Control Ition Protocol (reques	e 1 (78 or 802.11 cal-Link (ess Resolu	Fram 1EEE Logi Addr		
010 00 8e ef ed 9e 00 70 68 aa aa 03 00 00 00 06iiph 22 120 00 01 08 00 05 04 00 01 00 8e ef ed 9e 00 ac 10	î	1	0000-00-9-19	00 40 96 42 49 70		19.02.00.0	000 0		
120 00 01 08 00 05 04 00 01 00 Re eF ef 9e 00 at 10				03 00 00 00 08 0511	d 9e 00 70 68 aa aa (0 8e ef e	010 0		
				eF ed Se 00 an 10	0 06 04 00 01 00 Re /	0 01 08 0	20 0		
d Reset File: Kismet-Anr-01-2002-1 dump		met-Anr-01-2002-1 dump	eat File: Kisr	/ Be			tor		

Figure 6 (Ethereal with logs imported from Kismet)

a moste	n@viao	.bleepyou.	com:/home/mosten/TEMP	- • ×
File	Edit	Settings	Help	
-Networ SSII pal: 	·ks) .sade		T W Ch Data LLC Crypt Wk Flags A Y 08 14129 39646 14129 18 	-Info
r-Status Detect Loggir Captur Kismet	ted neu 19 data 19 jata 19 p. 1,4	w network a networks ackets fro	"palisade" bssid 00:40:96:29:28:AD WEP Y Ch 8 weak cisco n Prism/2	

Figure 4 (Kismet monitoring WEP enabled network)

Notice the "Crypt" field of figure 4. This field displays the actual number of WEP encrypted packets that have traveled from the 802.11b access point. 802.11b access points can be very noisy, sending broadcasts to wireless clients several times a second. These broadcasts are not WEP encrypted, numbers of which can be seen under the "Data" heading. Weak RC4 keys under the "Wk" heading are the significant field when attempting to break WEP security. Airsnort requires 1500-1800 weak (Wk) RC4 encrypted packets to extract the correct 128 WEP key. This would require approx. 4 million WEP encrypted packets.

File 1	Edit Settings Hel	p		_	_				
	A scan								
C	BSSID	Name	Last Seen	Last IV	Chan	Packets	Interesting		
00>	40.96.29.26.AD	palisade		28.00.1F	8	18	0		
-	3	Zart	Stop			Clear	J	~	

Figure 4 (AirSnort monitoring WEP encrypted network)

Conclusions and proposed possible solutions

First and foremost, WEP, although insecure, provides a significant deterrent to the casual easedropper. Consider that exploiting the weaknesses of WEP would require 8+ hours of sniffing and millions of packets of encrypted data.

Consider installing a firewall that separates your wireless access point from any internal network. This would reduce the risk of sensitive data being intercepted via sniffing, or exploits run on internal machines.

NoCatAuth (see resources) provides both user authentication and firewall capabilities for wireless networks, and is used extensively in the open wireless community. NoCatAuth is licensed under the GPL making source code available to the user.

Some of the key features of NoCatAuth:

Ouser Authentication
Ostatefull firewalling
Ocaching DNS server
Oquality of Service



Resources

Security of the WEP algorithm\u" (http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html) "NetStumbler\d \u"Ministumbler\u" (http://www.netstumbler.com/) Kismet (http://www.kismetwireless.net/) NoCatNet (http://nocat.net/) Ethereal (http://www.ethereal.com/)